Créer un compte Se connecter

Article Discussion Lire Modifier le code Afficher l'historique Rechercher

WIKIPÉDIA
L'encyclopédie libre

Navigation
Accueil
Portails thématiques
Article au hasard
Contact

Contribuer
Débuter sur Wikipédia
Aide
Communauté
Modifications récentes
Faire un don

Imprimer / exporter
Créer un livre
Télécharger comme PDF
Version imprimable

Outils
Pages liées
Suivi des pages liées
Importer un fichier
Pages spéciales
Adresse de cette version
Information sur la page
Élément sur Wikidata
Citer cette page

Autres langues
Afrikaans
العربية
Azərbaycanca
Беларуская
Български
Bosanski
Català
Čeština
Dansk
Deutsch
Ελληνικά
English
Esperanto
Español
Eesti
Euskara
فارسی
Suomi
Galego
עברית
Hrvatski
Magyar
Bahasa Indonesia
Italiano
日本語
Қазақша
한국어
Lietuvių
Latviešu

Secure Shell

(Redirigé depuis Secure shell)

Pour les articles homonymes, voir SSHD.

Secure Shell	
Fonction	Session à distance sécurisée
Sigle	SSH
Date de création	1995
Port	TCP/22
RFC	RFC 4251

modifier

Secure Shell (**SSH**) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un *sniffer* pour voir ce que fait l'utilisateur.

Le protocole **SSH** a été conçu avec l'objectif de remplacer les différents programmes rlogin, telnet, rcp, ftp et rsh.

Pile de protocoles

7. Application
6. Présentation
5. Session
4. Transport
3. Réseau
2. Liaison
1. Physique

Modèle Internet
Modèle OSI

modifier

Sommaire

1 Le protocole
2 Historique
3 SSH avec authentification par clés
4 Implémentations logicielles
5 Notes et références
6 Voir aussi
6.1 Articles connexes
6.2 Liens externes

Le protocole [modifier le code]

Le protocole **SSH** existe en deux versions majeures : la version 1.0 et la version 2.0.

- La première version permet de se connecter à distance à un ordinateur afin d'obtenir un shell ou ligne de commande. Cette version souffrait néanmoins de problèmes de sécurité dans la vérification de l'intégrité des données envoyées ou reçues, la rendant vulnérable à des attaques actives. En outre, cette version implémentait un système sommaire de transmission de fichiers, et du *port tunneling*.
- La version 2 qui était à l'état de *draft* jusqu'en janvier 2006 est déjà largement utilisée à travers le monde.

Cette version est beaucoup plus sûre au niveau cryptographique, et possède en plus un protocole de transfert de fichiers complet, le SSH file transfer protocol.

Habituellement le protocole SSH utilise le port TCP 22. Il est particulièrement utilisé pour ouvrir un shell sur un ordinateur distant. Peu utilisé sur les stations Windows (quoiqu'on puisse l'utiliser avec PuTTY, mRemote, cygwin ou encore OpenSSH), SSH fait référence pour l'accès distant sur les stations Linux et Unix.

SSH peut également être utilisé pour transférer des ports TCP d'une machine vers une autre, créant ainsi un tunnel. Cette méthode est couramment utilisée afin de sécuriser une connexion qui ne l'est pas (par exemple le protocole de récupérations de courrier électronique POP3) en la faisant transférer par le biais du tunnel chiffré SSH.

Il est également possible de faire plusieurs sauts entre consoles SSH, c'est-à-dire ouvrir une console sur un serveur, puis, de là, en ouvrir une autre sur un autre serveur.

Historique [modifier le code]

La première version de SSH (SSH-1) a été conçue par Tatu Ylönen, à Espoo, en Finlande en 1995. Il a créé le premier programme utilisant ce protocole et a ensuite créé une entreprise, SSH Communications Security pour exploiter cette innovation. Cette première version utilisait certains logiciels libres comme la bibliothèque Gnu libgmp, mais au fil du temps ces logiciels ont été remplacés par des logiciels propriétaires. SSH Communications Security a vendu sa licence SSH à F-Secure (anciennement connue sous le nom de Data Fellows).

La version suivante a été nommée SSH-2. Le groupe de recherche de l'IETF « secsh » a défini en janvier 2006 le standard Internet SSH-2, que l'on retrouve actuellement dans la plupart des implémentations. Cette version permet une compatibilité ascendante avec les implémentations du *draft* de SSH-2 qui étaient en version 1.99.

SSH avec authentification par clés [modifier le code]

Avec SSH, l'authentification peut se faire sans l'utilisation de mot de passe ou de phrase secrète en utilisant la

Македонски
Nederlands
Norsk bokmål
Polski
Português
Română
Русский
Simple English
Slovenčina
Slovenščina
Shqip
Српски / srpski
Svenska
ไทย
Türkçe
Українська
Tiếng Việt
Yorùbá
中文
Modifier les liens

cryptographie asymétrique. La clé publique est distribuée sur les systèmes sur lesquels on souhaite se connecter. La clé privée, qu'on prendra le soin de protéger par un mot de passe, reste uniquement sur le poste à partir duquel on se connecte. L'utilisation d'un « agent ssh (en) » permet de stocker le mot de passe de la clé privée pendant la durée de la session utilisateur.

Cette configuration profite aussi à SCP et à SFTP qui se connectent au même serveur **SSH**.

Implémentations logicielles [modifier le code]

- *OpenSSH*, le projet libre d'outils SSH. OpenSSH est l'implémentation ssh la plus utilisée, y compris par les distributions GNU/Linux.
- *Portable OpenSSH*, une implémentation OpenSSH multiplate-forme.
- *lsh*[1], une implémentation distribuée par le projet GNU selon les termes de la licence GNU GPL.
- *MacSSH*[2], une implémentation *lsh* pour Mac OS classic 68k et PPC.
- *FRESH*[3], une implémentation ssh en environnement JBoss.
- *SSHWindows*[4], une implémentation pour Windows non maintenue.
- *Dropbear*[5], une implémentation libre ayant pour but de remplacer OpenSSH sur les systèmes Unix ayant peu de ressources (processeur, mémoire, etc.) comme par exemple les systèmes embarqués.

Notes et références [modifier le code]

1. ↑ (en) Implémentation GNU
2. ↑ (en) MacSSH sur la plateforme SourceForge
3. ↑ (en) FRESH
4. ↑ (en) SSHWindows sur la plateforme SourceForge
5. ↑ (en) Dropbear

Voir aussi [modifier le code]

Articles connexes [modifier le code]

- Protocole de communication
- OpenSSH : Implémentation libre de SSH
- *SSH File Transfer Protocol* (soit *SSH FTP*) transfert de fichiers à travers SSH
- *Secure shell file system* (soit *SSHFS*) partage de systèmes de fichiers à travers SSH
- *Secure copy* : transfert de fichiers à travers SSH
- *Files transferred over shell protocol* (en) : transfert de fichiers à travers un shell SSH
- PuTTY - client SSH multi-OS
- WinSCP - client SFTP graphique pour Windows
- TTyEmulator - Émulateur de terminal propriétaire, en français sous Windows incluant un grand nombre de fonctionnalités.

Sur les autres projets Wikimedia :

Secure shell, sur Wikiversity

Liens externes [modifier le code]

- Catégorie SSH de l'annuaire dmoz
- (fr) Site Web d'OpenSSH
- RFC 4251 : Architecture générale du protocole
- RFC 4252 : Protocole d'authentification (PKI, par mot de passe ou par machine)
- RFC 4253 : Protocole de transport sécurisé (Chiffrement, Signature numérique, intégrité)
- RFC 4254 : Protocole de connexion (Port tunneling, Shell)

v · d · m	Couches du modèle OSI
7. Application	DHCP · DNS · FTP · Gopher · H.323 · HTTP · IMAP · IRC · NFS · NNTP · POP3 · RTSP · SILC · SIMPLE · SIP · SMTP · SNMP · SMB-CIFS · **SSH** · TCAP · Telnet · TFTP · VoIP · XMPP · WebDAV
6. Présentation	AFP · ASCII · ASN.1 · MIME · NCP · SSP · TDI · TLV · Unicode · UUCP · Vidéotex · XDR
5. Session	AppleTalk · DTLS · H.323 · RSerPool · SOCKS · TLS
4. Transport	DCCP · RSVP · RTP · SCTP · SPX · TCP · UDP
3. Réseau	ARP · BGP · Babel · BOOTP · CLNP · ICMP · IGMP · IPv4 · IPv6 · IPX · IS-IS · NetBEUI · OSPF · RARP · RIP · X.25
2. Liaison	Anneau à jeton · ARINC 429 · ATM · AFDX · Bitnet · CAN · Ethernet · FDDI · Frame Relay · HDLC · I²C · IEEE 802.3ad (LACP) · LLC · LocalTalk · MIL-STD-1553 · PPP · STP · Wi-Fi · X.21
1. Physique	4B5B · ADSL · BHDn · Bluetooth · Câble coaxial · Codage bipolaire · CSMA/CA · CSMA/CD · DSSS · E-carrier · EIA-232 · EIA-422 · EIA-449 · EIA-485 · FHSS · IEEE 1394 · HomeRF · IrDA · ISDN · Manchester · Manchester différentiel · Miller · MLT-3 · NRZ · NRZI · NRZM · Paire torsadée · PDH · SDH · SDSL · SONET · T-carrier · USB · VDSL · V.21-V.23 ·

	V.42-V.90 · Wireless USB · 10BASE-T · 10BASE2 · 10BASE5 · 100BASE-TX · 1000BASE-T
Articles liés	Pile de protocoles · Modèle Internet

v · d · m	**Schéma d'URI**
Officiel	aaa · aaas · acap · cap · cid · crid · data · dav · dict · dns · fax · file · ftp · geo · go · gopher · h323 · http · https · im · imap · info · ldap · mailto · mid · news · nfs · nntp · pop · pres · rtsp · sip · sips · snmp · tag · tel · telnet · urn · wais · xmpp
Non-officiel	about · afp · aim · apt · bzr · callto · coffee · cvs · daap · ed2k · feed · fish · gg · git · gizmoproject · iax2 · irc · ircs · itms · ldaps · magnet · mms · msnim · rsync · secondlife · skype · spotify · **ssh** · svn · sftp · smb · sms · steam · view-source · vzochat · webcal · winamp · wyciwyg · xfire · ymsgr

Portail de la sécurité informatique **Portail de la cryptologie**

Catégories : Protocole de communication chiffrée | Logiciel d'administration sécurisée à distance | Protocole réseau sur la couche application | Standard Internet

Dernière modification de cette page le 21 avril 2014 à 11:15.

Droit d'auteur : les textes sont disponibles sous licence Creative Commons paternité partage à l'identique ; d'autres conditions peuvent s'appliquer. Voyez les conditions d'utilisation pour plus de détails, ainsi que les crédits graphiques. En cas de réutilisation des textes de cette page, voyez comment citer les auteurs et mentionner la licence.
Wikipedia® est une marque déposée de la Wikimedia Foundation, Inc., organisation de bienfaisance régie par le paragraphe 501(c)(3) du code fiscal des États-Unis.

Politique de confidentialité À propos de Wikipédia Avertissements Développeurs Version mobile